Amendments to the Claims

1. (CURRENTLY AMENDED) A logic circuit for multiplication of an ~~(m × n)~~ matrix by a ~~(1 × n)~~ or by a ~~(m × 1)~~ matrix, where m is a number of rows and n is a number of columns, and wherein each successive row m of n elements is a predetermined row permutation of a preceding row, the circuit comprising:

n multiplication circuits ~~(60…63)~~ each having an input and an output which returns the value of said input multiplied by a predetermined multiplicand;

n logic circuits, ~~(70…73)~~ each for executing a predetermined logical combination of a first input and a second input to provide a logical output, the first input being coupled to the output of a corresponding one of the n multiplication circuits;

n registers ~~(80…83)~~ for receiving said logical output;

feedback logic for routing the contents of each register to a selected one of the second inputs in accordance with a feedback plan that corresponds to the predetermined row permutation; and

control means for successively providing as input to each of the n multiplication circuits each element in the ~~(1 × n)~~ or ~~(m × 1)~~ matrix.

2. (ORIGINAL) The logic circuit of claim 1 in which the feedback logic provides a feedback plan corresponding to said predetermined row permutation that is a row shift.

3. (ORIGINAL) The logic circuit of claim 2 in which the row shift is a single element right shift.

4. (ORIGINAL) The logic circuit of claim 1 in which the n logic circuits are each adapted to execute an XOR-combination of said first input and said second input.

5. (ORIGINAL) The logic circuit of claim 1 in which each of the predetermined multiplicands corresponds to one of the elements in the AES Rijndael MixColumns transform function.

6. (ORIGINAL) The logic circuit of claim 5 in which the number m = 4, the number n = 4, the multiplicand for the first multiplication circuit = 02, the multiplicand for the second multiplication circuit = 03, the multiplicand for the third multiplication circuit = 01, and the multiplicand for the fourth multiplication circuit = 01.

7. (ORIGINAL) The logic circuit of claim 5 in which the number m = 4, the number n = 4, the multiplicand for the first multiplication circuit = 0E, the multiplicand for the second multiplication circuit = 0B, the multiplicand for the third multiplication circuit = 0D, and the multiplicand for the fourth multiplication circuit = 09.

8. (CURRENTLY AMENDED) The logic circuit of ~~claim 6 or claim 7~~ claim 6in which the four multiplicands are switchable between the values in ~~claim 6 and the values in claim 7~~claim 6.

9. (ORIGINAL) The logic circuit of claim 1 in which the control means is adapted to successively provide as input to each of the n multiplication circuits each successive element in the (1 × n) or (m × 1) matrix over each of n or m cycles of operation respectively.

10. (ORIGINAL) The logic circuit of claim 1 in which each of the n multiplication circuits, each of the n logic circuits, and each of the n registers are at least eight bits wide.

11. (ORIGINAL) The logic circuit of claim 1 in which the control means further includes means for providing as output from said logic circuit the contents of the n registers after each *n*th cycle.

12. (ORIGINAL) The logic circuit of claim 1 in which the control means further includes means for resetting each of the registers prior to the first calculation cycle.

13. (ORIGINAL) The logic circuit of claim 1 in which each successive row m of n elements is a predetermined row permutation of the immediately preceding row.

14. (CURRENTLY AMENDED) An AES MixColumns transform circuit incorporating the logic circuit of any one of claims 1 to 13.

15. (CURRENTLY AMENDED) An AES encryption and/or decryption engine incorporating the logic circuit of ~~any one of claims 1 to 13~~claim 1 for performing the MixColumns transform.

16. (ORIGINAL) Apparatus substantially as described herein with reference to the accompanying drawings.